arXiv:math/0002139v2 [math.NT] 4 Jan 2001

THE DISTRIBUTION OF SPACINGS BETWEEN THE FRACTIONAL PARTS OF $n^2\alpha$

ZEÉV RUDNICK[(1)], PETER SARNAK[(2)] AND ALEXANDRU ZAHARESCU

1. Introduction

Fix an irrational number α. The problem of the distribution of the local spacings between the members of the sequence $n^2\alpha \mod 1$, $1 \le n \le N$, has received attention recently (see [2, 5, 14]). It arises for example in the study of the local spacing distributions between the eigenvalues of special Hamiltonians. We order the above numbers in $[0,1)$ as

$$0 \le \beta_1 \le \beta_2 \le \cdots \le \beta_N < 1 \tag{1.1}$$

and set $\beta_{N+j} = \beta_j$. The k-th consecutive spacing measure is defined to be the probability measure on $[0,\infty)$ given by

$$\mu_k(N,\alpha) := \frac{1}{N}\sum_{j=1}^{N} \delta_{N(\beta_{j+k}-\beta_j)} \tag{1.2}$$

where δ_x is a unit delta mass at x. The problem is to understand the behavior of these measures as $N \to \infty$ and in particular their dependence on the diophantine approximations to α.

We say α is of type K if there is $c_\alpha > 0$ such that $|\alpha - \frac{a}{q}| \ge c_\alpha q^{-K}$ for all relatively prime integers a and q. It is easy to see that if α is not of type 3 then there is a subsequence $N_j \to \infty$ for which the measures $\mu_k(N_j,\alpha)$ converge to a measure supported on $\mathbf{N} = \{0,1,2,\cdots\}$. On the other hand numerical experiments [5] indicate that for $\alpha = \sqrt{2}$ these k-th consecutive spacings behave like what one typically gets for spacings when placing N numbers in $[0,1]$ uniformly and independently at random [10]. That is $\mu_k(N,\sqrt{2})$ appears to converge to $\mu_k := \frac{x^k}{k!}e^{-x}dx$.

Date: February 1, 2008.

(1) Supported in part by a grant from the U.S.-Israel bi-national Science Foundation.

(2) Supported in part by a grant from the U.S.-Israel bi-national Science Foundation and the NSF.

A standard approach to the analysis of the consecutive spacing is via local m-level correlations. These are defined as follows: As test functions we use functions $f(x_1, x_2, \cdots, x_m)$ which are symmetric in $(x_1, x_2, \cdots, x_m)$ and which are functions of the difference of the coordinates, that is $f(x + (t, t, \cdots, t)) = f(x)$ for all $t \in \mathbf{R}$. We assume further that f is local, that is it is compactly supported modulo the diagonal. We will call these *admissible* test functions. Define the correlations

$$R^{(m)}(N, \alpha, f) := \frac{1}{N} \sum_{1 \leq j_1 < \ldots < j_m \leq N} f(N(\beta_{j_1}, \cdots, \beta_{j_m})). \tag{1.3}$$

Note that $R^{(m)}$ is not a *probability* density and it may well tend to infinity as $N \to \infty$ (think of the case when α is rational). In the case that the β's in (1.1) come from a random choice of points in $[0, 1)$ these correlations satisfy

$$R^{(m)}(N, f) \to \int_{0 \leq x_2 \leq \ldots \leq x_m} f(0, x_2, \cdots, x_m) dx_2 \cdots dx_m. \tag{1.4}$$

We say that $n^2\alpha \mod 1$, $n \leq N$, is Poissonian if for all $m \geq 2$ and f as above

$$R^{(m)}(N, \alpha, f) \to \int_{0 \leq x_2 \leq \ldots \leq x_m} f(0, x_2, \cdots, x_m) dx_2 \cdots dx_m \tag{1.5}$$

as $N \to \infty$.

As with the method of moments in convergence of measures, if the m-level correlations are Poissonian then the consecutive spacing measures $\mu_k(N, \alpha)$ converge to μ_k. Thus Poissonian in the sense of (1.5) (i.e. for correlations) implies that as far as local spacings go, the numbers behave randomly. We will also consider cases where (1.5) holds along a subsequence $N_j \to \infty$, in such a case we say that $n^2\alpha \mod 1$, $1 \leq n \leq N$ is Poissonian on a subsequence.

The results below lead us to the following

Conjecture: *If α is of type $2+\epsilon$ for every $\epsilon > 0$ and the convergents $\frac{a}{q}$ to α satisfy $\lim_{q \to \infty} \frac{\log \tilde{q}}{\log q} = 1$, where $\tilde{q}$ is the square free part of q, then $n^2\alpha \mod 1$ is Poissonian.*

We note that almost all α (for Lebesgue measure) satisfy the hypothesis in the Conjecture and that assuming some standard conjectures in diophantine analysis any real algebraic irrationality satisfies these hypotheses (see Appendix A).

Unfortunately the methods of this paper appear not to be powerful enough to prove anything for the numbers α in the Conjecture. They require that α have somewhat better approximations by rationals. One of our main results gives conditions on the diophantine approximations to α which ensure that $n^2\alpha \mod 1$ is Poissonian along a subsequence. In particular this allows us to conclude that for the topologically generic α (i.e. in the sense of Baire) $n^2\alpha \mod 1$ is Poissonian along a subsequence. On the other hand the naive expectation that for any irrational α, $n^2\alpha \mod 1$ is Poissonian along a subsequence, fails dramatically. The source of this phenomenon is large square factors in the denominator of the convergents to α. We will exhibit an α for which the 5-level correlations go to infinity as $N \to \infty$. We also provide an α of type less than three and a sequence of integers $\{N_j\}_{j=1}^{\infty}$ along which the 5-level correlations diverge to infinity.

The precise statements are as follows:

Theorem 1. *Let $\alpha \in \mathbf{R}$. Suppose there are infinitely many rationals b_j/q_j, with q_j* prime*, satisfying*

$$\left|\alpha - \frac{b_j}{q_j}\right| < \frac{1}{q_j^3} .$$

Then there is a subsequence $N_j \to \infty$ with $\frac{\log N_j}{\log q_j} \to 1$ for which (1.5) holds for all $m \geq 2$ and all f. That is to say $n^2\alpha \mod 1$ is Poissonian along this subsequence.

With a lot more work concerning the exponential sums discussed in Section 9, for general moduli q, we can relax the condition that q_j be prime in Theorem 1. In fact we can prove the following (we do not go into the proof in this paper) which shows that for such approximants the size of the square free parts $\tilde{q}_j$ of q_j is decisive.

Theorem 1': *Let α be an irrational for which there are infinitely many rationals b_j/q_j satisfying*

$$\left|\alpha - \frac{b_j}{q_j}\right| < \frac{1}{q_j^3} .$$

Then the following are equivalent :

(i) There is a subsequence $N_j \to \infty$ with $\frac{\log N_j}{\log q_j} \to 1$ such that $n^2\alpha \mod 1$ is Poissonian along N_j.

(ii)

$$\lim_{j\to\infty} \frac{\log \tilde{q}_j}{\log q_j} = 1 .$$

As to the divergence of correlations we have:

Theorem 2. *(a) There is an irrational α and a test function f such that*

$$R^{(5)}(N,\alpha,f) \gg N^{\frac{1}{4}}(\log N)^{-5}, \ \ as \quad N \to \infty \ .$$

(b) For every $\sigma > 23/8$ there is an α of type σ and a test function f such that

$$\overline{\lim_{N\to\infty}} R^{(5)}(N,\alpha,f) = \infty \ .$$

The test functions f in Theorem 2 are nonnegative and are supported in a neighborhood of 0 (modulo the diagonal) and the source of the divergence is that there are zero density, but non-negligible, clusters among the numbers $n^2\alpha \mod 1$, $n \leq N$.

We note that these clusters which spoil the correlations do not have the same effect on the probability measures $\mu_k(N,\alpha)$. So it is quite possible for example that the α in part (b) of Theorem 2 has its $\mu_k(N,\alpha)$ measures converge to the Poissonian μ_k. We have chosen in this paper to call $n^2\alpha \mod 1$ Poissonian if the strongest behavior holds - that is the correlations are Poissonian.

The proofs of the above theorems are based on the following closely related diophantine problem: Consider the spacing distributions (normalized to mean spacing 1 as before) of the numbers $\{bn^2/q\}$, $n \leq N$, or what is the same, the spacing distribution of the integers

$$n^2 b \mod q, \qquad 1 \leq n \leq N. \tag{1.6}$$

Here q is prime ($q \to \infty$), b is any number not divisible by q and N is in the range $[q^{1/2+\epsilon}, \frac{q}{\log q}]$ for some $\epsilon > 0$. The reason for this range for N is that if $N \leq \sqrt{q}$ and say $b = 1$ then the spacing distributions may be easily determined (since $n^2 < q$ for $n \leq N \leq \sqrt{q}$) and are certainly nonrandom. Similarly if $N = q$ then the sequence in (1.6) consists of all the quadratic residues (or non-residues) and hence the spacings are integers and so cannot follow a Poissonian law. In fact the limiting spacing distributions of $\mu_k(q,q,b)$ were determined by Davenport [6, 7]. So it is only in the range $N \in [q^{1/2+\epsilon}, \frac{q}{\log q}]$ that we can hope for randomization. The following Theorem shows that indeed, to a certain extent, this is the case.

Let $R^{(m)}(N, b/q, f)$ denote the scaled m-level correlations for the sequence (1.6).

Theorem 3. *Fix $m \geq 2$, f and $\delta > 0$. Then as $q \to \infty$, q prime*

$$R^{(m)}(N, b/q, f) \to \int_{0\leq x_2 \leq \ldots \leq x_m} f(0, x_2, \cdots, x_m) dx_2 ... dx_m$$

uniformly for $(b,q)=1$ *and* $q^{1-\frac{1}{2m}+\delta} \le N \le \frac{q}{\log q}$.

A crucial ingredient in our proof of Theorem 3 is the Riemann Hypothesis for curves (of arbitrary large genus) over finite fields (Weil [15]).

In the range in which Theorem 3 applies it gives Poisson statistics and Theorem 3 easily yields Theorem 1. For $m \ge 3$ it is not possible to extend the range of N in Theorem 3 much further. The reason is related to the previous divergence of correlations phenomenon. For suitable b (depending on q) there will be large clusters among the numbers $n^2 b \pmod q$, $n \le N$. This is highlighted by the following Theorem.

Theorem 4. *Fix* $m \ge 3$ *and* $\delta > 0$. *Then there is a test function* f *such that for* $q^{\frac{1}{2}} \le N \le q^{\frac{m}{m+2}-\delta}$,

$$\lim_{q\to\infty} \max_{(b,q)=1} R^{(m)}(N, b/q, f) = \infty \, .$$

Acknowledgment: We would like to thank E. Bombieri for his help with the application of the ABC conjecture described in Appendix A. We also thank the referee for suggesting a stronger version of Theorem 2 (a) with a simpler proof than our original one.

2. A comparison lemma

We will need to deal with the following situation: We are given two families of sequences $\mathcal{N} = \{x_N(n) : n \le N\}$ and $\mathcal{N}' = \{x'_N(n) : N \le N\}$ in $[0,1)$ and we wish to compare the limiting correlation functions of these two families, seeking to show that if the correlations exist for one sequence then they exist for the other, or they diverge for one if they do for the other. We show that it can be done if the two sequences are close in a suitable sense. We define the scaled distance between the sequences to be

$$\epsilon(\mathcal{N}, \mathcal{N}') := N \max_{n\le N} |x_N(n) - x'_N(n)| \, .$$

A general method for carrying out the comparison is formalized in the following:

Lemma 5 (Comparison Lemma)**.** *Assume that* $\mathcal{N}, \mathcal{N}' \subset [0,1)$ *are two families of sequences with* $\epsilon(\mathcal{N}, \mathcal{N}') \to 0$ *as* $N \to \infty$. *Then for all smooth test functions* f, *we have*

$$\left| R^{(k)}(\mathcal{N}, f) - R^{(k)}(\mathcal{N}', f) \right| \le R^{(k)}(\mathcal{N}, f_+)\epsilon(\mathcal{N}, \mathcal{N}')$$

for N *sufficiently large, where* $f_+ \ge 0$ *is a smooth admissible test function (depending only on* f*).*

Proof. For notational simplicity, we will do the case of pair correlation ($k = 2$). Our test function $f \neq 0$ can then be written as $f(x_1, x_2) = g(x_1 - x_2)$ for some $g \in C_c^\infty(\mathbf{R})$, say g supported inside $[-\rho, \rho]$. Let $g_+ \geq 0$ be smooth, compactly supported and such that g_+ is constant on $[-2\rho, 2\rho]$, where it equals $\max |g'|$. Set $f_+(x_1, x_2) := 2g_+(x_1 - x_2)$. For further notational simplicity also set $\delta_{m,n} := x_N(m) - x_N(n)$ and $\delta'_{m,n} := x'_N(m) - x'_N(n)$.

By the mean value theorem we have

$$\begin{aligned} R^{(2)}(\mathcal{N}, f) - R^{(2)}(\mathcal{N}', f) &= \frac{1}{N} \sum_{1 \leq m < n \leq N} g(N\delta_{m,n}) - g(N\delta'_{m,n}) \\ &= \frac{1}{N} \sum_{1 \leq m < n \leq N} g'(N\xi_{m,n}) \cdot N(\delta_{m,n} - \delta'_{m,n}) \end{aligned}$$

where $\xi_{m,n}$ lies between $\delta_{m,n}$ and $\delta'_{m,n}$.

For the difference $R^{(2)}(f, \mathcal{N}) - R^{(2)}(f, \mathcal{N}')$ to contain a nonzero contribution from the term indexed by the pair (m, n), we must have at least one of $N\delta_{m,n}$ or $N\delta'_{m,n}$ lying in $\operatorname{supp} g \subset [-\rho, \rho]$. Now $N\xi_{m,n}$ is within $2\epsilon(\mathcal{N}, \mathcal{N}')$ of both $N\delta_{m,n}$ and $N\delta'_{m,n}$, which implies that *both* lie in $[-2\rho, 2\rho]$, as does $\xi_{m,n}$ if N is sufficiently large so that $2\epsilon(\mathcal{N}, \mathcal{N}') < \rho$. Since g_+ is constant on $[-2\rho, 2\rho]$ we find that $g_+(\xi_{m,n}) = g_+(N\delta_{m,n})$.

Thus we get

$$\begin{aligned} |R^{(2)}(\mathcal{N}, f) - R^{(2)}(\mathcal{N}', f)| &\leq \frac{1}{N} \sum_{1 \leq m < n \leq N} g_+(N\delta_{m,n}) \cdot 2\epsilon(\mathcal{N}, \mathcal{N}') \\ &= R^{(2)}(\mathcal{N}, f_+)\epsilon(\mathcal{N}, \mathcal{N}') \end{aligned}$$

as required. □

3. Derivation of Theorem 1

As an immediate application of the comparison lemma, we derive Theorem 1 from Theorem 3.

Fix α. Suppose there are infinitely many rationals b_j/q_j with q_j prime, satisfying

$$|\alpha - \frac{b_j}{q_j}| < \frac{1}{q_j^3}.$$

We let $N_j = [\frac{q_j}{\log q_j}]$, where $[.]$ denotes the integer part function. Fix an $m \geq 2$ and a test function f as above. We need to show that

$$\lim_{j \to \infty} R^{(m)}(N_j, \alpha, f) = \int_{0 \leq x_2 \leq \cdots \leq x_m} f(0, x_2, \cdots, x_m) dx_2 \cdots dx_m.$$

By Theorem 3 applied to $q = q_j, b = b_j$ and $N = N_j$ we know that

$$\lim_{j\to\infty} R^{(m)}(N_j, b_j/q_j, f) = \int_{0\le x_2\le\cdots\le x_m} f(0, x_2, \cdots, x_m)dx_2\cdots dx_m$$

We use the comparison principle to estimate the difference:

$$|R^{(m)}(N_j, \alpha, f) - R^{(m)}(N_j, b_j/q_j, f)| .$$

Take $\mathcal{N}_j' = \{\{\alpha n^2\} : n \le N_j\}$ and $\mathcal{N}_j = \{\{b_j n^2/q_j\} : n \le N_j\}$. By lemma 5,

$$|R^{(m)}(\mathcal{N}_j', f) - R^{(m)}(\mathcal{N}_j, f)| \le R^{(m)}(\mathcal{N}_j, f_+)\epsilon(\mathcal{N}_j, \mathcal{N}_j') \tag{3.1}$$

for some admissible test function $f_+ \ge 0$. We have

$$|\{\alpha n^2\} - \{\frac{b_j}{q_j}n^2\}| \le |\alpha - \frac{b_j}{q_j}|n^2 \le \frac{N_j^2}{q_j^3} \sim \frac{1}{N_j(\log N_j)^3}$$

and thus

$$\epsilon(\mathcal{N}_j, \mathcal{N}_j') = N_j \max_{n\le N_j} |\{\alpha n^2\} - \{\frac{b_j}{q_j}n^2\}| \le \frac{1}{(\log N_j)^3} \to 0 .$$

By Theorem 3, $R^{(m)}(\mathcal{N}_j, f_+)$ is bounded (it converges as $j \to \infty$). Thus we use (3.1) to deduce that

$$|R^{(m)}(N_j, \alpha, f) - R^{(m)}(N_j, b_j/q_j, f)| \to 0$$

which gives Theorem 1. □

4. A divergence principle

We present a mechanism that ensure divergence of high correlations of the sequence $\{bn^2/q\}$: The presence of larges square factors in q.

Lemma 6. *Let $q = uv^2$ with $v > q^\delta$ for some $\delta > 0$, let $\eta > 1 - \delta$ and suppose that* $\log N/\log q > \eta$. *Let $f \ge 0$ be a* positive *admissible test function which is non-vanishing at the origin. Then for all b,*

$$R^{(m)}(N, \frac{b}{q}, f) \gg \frac{1}{N} f(0)(\frac{Nv}{q})^m . \tag{4.1}$$

In particular $R^{(m)}(N, b/q, f)$ will diverge to infinity for m sufficiently large in terms of δ and η.

Proof. Write $f(x_1, \ldots, x_m) = g(x_1 - x_2, \ldots x_{m-1} - x_m)$ for $g \in C_c(\mathbf{R}^{m-1})$, $g \ge 0$, $g(0) \ne 0$. Then

$$R^{(m)}(N, \frac{b}{q}, f) = \frac{1}{N} \sum_{1\le n_1<\cdots<n_m\le N} g(\ldots, N\{\frac{bn_j^2}{q}\} - N\{\frac{bn_{j+1}^2}{q}\}, \ldots)$$

Since $g \geq 0$, we may count only the contribution of those $(n_1, \dots, n_m)$ (n_j distinct) for which all the components $n_1, \dots, n_m$ are divisible by uv. There are $\gg [N/uv]^m = [Nv/q]^m$ such m-tuples. If $n = uvn'$ then since $q = uv^2$ we have

$$\{\frac{bn^2}{q}\} = \{bu(n')^2\} = 0$$

and so we find

$$R^{(m)}(N, \frac{b}{q}, f) \gg \frac{1}{N} f(0)(\frac{Nv}{q})^m \ .$$

Since $v > q^\delta$ and $N \gg q^\eta$ with $\eta > 1 - \delta$, this gives $R^{(m)}(N, \frac{b}{q}, f) \gg q^s$ with

$$s = \eta(m-1) + m\delta - m = m(\eta - (1-\delta)) - \eta$$

which is positive if $m > \eta/(\eta - (1-\delta)) > 0$. Thus for m sufficiently large, $R^{(m)}(N, b/q, f)$ will diverge in these ranges. □

5. Proof of Theorem 4

Fix $m \geq 2$, some small $\delta > 0$, and let N, q be large such that $q^{1/3} \leq N \leq q^{m/(m+2)-\delta}$. Let $f \geq 0$ is an admissible test function, $f(0) \neq 0$, and $f_+ \geq f$ the smooth majorant appearing in Lemma 5. We want to show that there exists $b < q$ coprime to q such that $R^{(m)}(N, b/q, f_+)$ is large.

We first produce q' which is a square, $q' = v^2$, coprime to q, such that

$$qq' \asymp N^3(\log N)^3 \ . \tag{5.1}$$

To do so, find v in the interval

$$J = \left[\sqrt{\frac{N^3 \log^3 N}{q}}, 2\sqrt{\frac{N^3 \log^3 N}{q}}\right]$$

which is coprime to q. Note that $N^3 \log^3 N/q \gg (\log q)^3$ since $N \geq q^{1/3}$ and so the existence of such numbers v is assured for any q sufficiently large. Indeed, if q is sufficiently large then in any interval $[x, 2x]$ with $x \gg (\log q)^{3/2}$ there is a prime ℓ not dividing q, since otherwise q would be divisible by all primes in the interval and consequently $\log q$ would be at least as large as $\sum_{x \leq p \leq 2x} \log p \sim x$ which contradicts $x \gg (\log q)^{3/2}$.

We now put $q' = v^2$. Thus $(q', q) = 1$ and (5.1) holds. Because $q' = v^2$ is a square, we may use the divergence principle (4.1) to see

that for all b' we have

$$R^{(m)}(N, \frac{b'}{q'}, f) \gg \frac{1}{N}(\frac{N}{v})^m$$

Since $v = \sqrt{q'} \ll \sqrt{N^3 \log^3 N/q}$, we find that for all b'

$$R^{(m)}(N, \frac{b'}{q'}, f) \gg \frac{N^{m-1}q^{m/2}}{N^{3m/2}(\log N)^{3m/2}} = \frac{q^{m/2}}{N^{m/2+1}(\log N)^{3m/2}} .$$

Now use $q^{1/3} \leq N \leq q^{m/(m+2)-\delta}$ to find that for some $C > 0$,

$$R^{(m)}(N, \frac{b'}{q'}, f) \geq Cq^{\delta(m/2+1)}(\log q)^{-3m/2} \tag{5.2}$$

uniformly in b' if $q > q_0$. Since $\delta > 0$, this diverges with q.

Because q, q' are coprime, there are $0 < b < q$, $0 < b' < q'$ so that $bq' - b'q = 1$ and so

$$|\frac{b}{q} - \frac{b'}{q'}| = \frac{1}{qq'} \asymp \frac{1}{N^3 \log^3 N} .$$

By the comparison principle (lemma 5), the two sequences $\mathcal{N} = \{\{bn^2/q\} : n \leq N\}$ and $\mathcal{N}' = \{\{b'n^2/q'\} : n \leq N\}$ satisfy

$$|R^{(m)}(N, \frac{b}{q}, f) - R^{(m)}(N, \frac{b'}{q'}, f)| \leq \epsilon(\mathcal{N}, \mathcal{N}')R^{(m)}(N, \frac{b}{q}, f_+) \tag{5.3}$$

where f_+ is a majorant for f, and in particular nonvanishing at the origin. Moreover

$$\begin{aligned} \epsilon(\mathcal{N}, \mathcal{N}') &= N \max_{n \leq N} |\{\frac{bn^2}{q}\} - \{\frac{b'n^2}{q'}\}| \leq |\frac{b}{q} - \frac{b'}{q'}|N^3 \\ &\leq \frac{1}{(\log N)^3} \ll \frac{1}{(\log q)^3} \end{aligned} \tag{5.4}$$

We claim that

$$R^{(m)}(N, \frac{b'}{q'}, f_+) \geq \frac{C}{3}q^{\delta(m/2+1)}(\log q)^{-3m/2}$$

Indeed, assuming otherwise we have from (5.3) and (5.4) that

$$|R^{(m)}(N, \frac{b}{q}, f) - R^{(m)}(N, \frac{b'}{q'}, f)| = o(q^{\delta(m/2+1)}(\log q)^{-3m/2})$$

which together with (5.2) forces $R^{(m)}(N, b/q, f) > \frac{C}{3}q^{\delta(m/2+1)}(\log q)^{-3m/2}$. However, since $f_+ \geq f \geq 0$ we find that

$$R^{(m)}(N, \frac{b}{q}, f_+) \geq R^{(m)}(N, \frac{b}{q}, f) > \frac{C}{3}q^{\delta(m/2+1)}(\log q)^{-3m/2}$$

contradicting our assumption. □

6. Preliminaries on continued fractions

We recall the standard notions of the theory of continued fractions (see e.g. [11]).

Given integers $a_0 \in \mathbf{Z}$, $a_1, a_2, \cdots \geq 1$, one defines integers p_m, q_m by the recursion ($m \geq 1$):

$$p_m = a_m p_{m-1} + p_{m-2}$$
$$q_m = a_m q_{m-1} + q_{m-2}$$

with $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$, $q_0 = 1$. These satisfy the relations

$$p_m q_{m-1} - p_{m-1} q_m = (-1)^{m-1}$$

and

$$p_m q_{m-2} - p_{m-2} q_m = (-1)^m a_m \ .$$

The finite continued fraction

$$[a_0; a_1, \ldots, a_m] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_m}}}}$$

is then p_m/q_m.

The infinite simple continued fraction $[a_0; a_1, a_2, \ldots]$ is the limit of the "convergents" p_m/q_m. Every irrational α has a unique continued fraction expansion.

The convergents give very good rational approximations to α: We have

$$\frac{1}{2}\frac{1}{q_m q_{m+1}} < |\alpha - \frac{p_m}{q_m}| < \frac{1}{q_m q_{m+1}} \ .$$

The convergents p_m/q_m are the "best" rational approximations to α, in the following senses: If p/q satisfies $|\alpha - p/q| < 1/2q^2$ then $p/q = p_m/q_m$ for some m. Moreover, for $m > 1$, if $0 < q \leq q_m$ and $p/q \neq p_m/q_m$ then $|\alpha - p/q| > |\alpha - p_m/q_m|$.

7. Proof of Theorem 2(a)

7.1. **Constructing α.** We want to find an irrational α such that

$$R^{(5)}(\alpha, N) \gg \frac{N^{1/4}}{(\log N)^5} \ . \tag{7.1}$$

The construction below is due to the referee, who strengthened and considerably simplified our original argument.

We construct α by means of its continued fraction expansion, by inductively finding $a_0, a_1, \dots, a_m$ so that the denominators q_m of the convergents are *squares*: $q_m = v_m^2$.

To do so, define pairs of integers (r_m, v_m) by $r_{-1} = v_{-1} = 0$, $r_0 = v_0 = 1$, $r_1 = v_1 = 1$ and for $m \geq 1$

$$v_{m+1} = r_m v_m^2 + v_{m-1}, \qquad r_{m+1} = [\log v_{m+1}] \tag{7.2}$$

Now set $a_0 = 1$, and for $m \geq 0$

$$a_{m+1} = r_m^2 v_m^2 + 2 r_m v_{m-1}$$

Let $\alpha = [a_0; a_1, a_2, \dots] = [1; 1, 3, 6, \dots]$.

We claim that the denominator q_m of convergent to α equals v_m^2. To see this, use induction: By the recursion for the convergents, $q_{m+1} = a_{m+1} q_m + q_{m-1}$ and by induction

$$\begin{aligned} q_{m+1} &= a_{m+1} v_m^2 + v_{m-1}^2 \\ &= (r_m^2 v_m^2 + 2 r_m v_{m-1}) v_m^2 + v_{m-1}^2 \\ &= (r_m v_m^2 + v_{m-1})^2 = v_{m+1}^2 \end{aligned}$$

as required.

Note also that from the recursion (7.2),

$$q_{m+1} \sim r_m^2 q_m^2 \sim q_m^2 (\log q_m)^2$$

Thus α is of type $3 + \epsilon$, for all $\epsilon > 0$.

Now we want to show that $R^{(5)}(\alpha, N) \gg N^{1/4}/(\log N)^5$. Pick m so that $q_m \leq N < q_{m+1}$. We will replace the sequence of fractional parts $\mathcal{N} = \{\{\alpha n^2\} : n \leq N\}$ by a different sequence depending on the size of N relative to q_m.

7.2. **Case 1: Assume that $q_m^{4/3} \leq N < q_{m+1}$.** Recall that $q_{m+1} \gg q_m^2 \log q_m$ and so this range is nonempty. Replace $\mathcal{N}$ by the sequence $\mathcal{N}' = \{x_n' : n \leq N\}$ where $x_n' = \{p_{m+1} n^2 / q_{m+1}\}$. These two sequences have asymptotically equal correlations since

$$|x_n - x_n'| \leq |\alpha - \frac{p_{m+1}}{q_{m+1}}| n^2 < \frac{N^2}{q_{m+1} q_{m+2}} \ll \frac{N^2}{r_{m+1}^2 q_{m+1}^3} \ll \frac{1}{N (\log N)^2}$$

since $q_{m+1} > N$ and $r_{m+1} = [\log q_{m+1}] \gg \log N$. Thus by the comparison principle (lemma 5), it suffices to work with the new sequence $\mathcal{N}'$.

By the divergence principle (see (4.1)), since $q_{m+1} = v_{m+1}^2$, if the test function f is nonvanishing at the origin we find that

$$R^{(5)}(\mathcal{N}', f) \gg \frac{1}{N} (\frac{N}{v_{m+1}})^5 = \frac{N^4}{q_{m+1}^{5/2}} \gg \frac{N^4}{r_m^5 q_m^5} \ .$$

Since $q_m \ll N^{3/4}$ and $r_m \sim \log N$ we find that

$$R^{(5)}(\mathcal{N}', f) \gg N^{1/4}(\log N)^{-5}$$

proving (7.1) when $q_m^{4/3} < N < q_{m+1}$.

7.3. **Case 2:** $q_m \leq N < q_m^{4/3}$**.** Set

$$M = \frac{q_m^{3/2}}{N^{1/2}}$$

Note that since $q_m \leq N < q_m^{4/3}$, M lies between $N^{5/8}$ and N. We replace $\mathcal{N}$ by the sequence $\mathcal{N}'' = \{x_n'' : n \leq N\}$ where

$$x_n'' = \begin{cases} \{\frac{p_m}{q_m} n^2\}, & n \leq M \\ x_n = \{\alpha n^2\}, & M < n \leq N \end{cases}$$

To check that correlations of $\mathcal{N}$ and $\mathcal{N}''$ are asymptotically equal, we need to see that $|x_n - x_n''| = o(1/N)$. For $n > M$ this certainly holds, while for $n \leq M$ we have

$$|x_n - x_n''| \leq |\alpha - \frac{p_m}{q_m}| n^2 \leq \frac{M^2}{q_m q_{m+1}}$$

Now use $q_{m+1} \gg r_m^2 q_m^2$ and since $q_m \sim (M^2 N)^{1/3}$ and $r_m \gg \log N$, we have

$$q_m q_{m+1} > r_m^2 q_m^3 \gg (\log N)^2 M^2 N$$

which gives $|x_n - x_n''| \ll 1/N(\log N)^2$ as required.

Now we study the sequence $\mathcal{N}''$. The number 0 occurs in $\mathcal{N}''$ if $n \leq M$ is a multiple of v_m: $n = v_m n'$, since then $x_n'' = \{\frac{p_m}{q_m} n^2\} = \{p_m (n')^2\} = 0$. Thus $\vec{0}$ occurs as a difference of 5-tuples of elements of $\mathcal{N}''$ at least $\gg [M/v_m]^5$ times. Thus if the origin lies in the support of the test function f then

$$R^{(5)}(\mathcal{N}'', f) \gg \frac{1}{N}(\frac{M}{v_m})^5 = \frac{M^5}{N q_m^{5/2}}$$

Since $M^2 = q_m^3/N$, and $N < q_m^{4/3}$ we get

$$R^{(5)}(\mathcal{N}'', f) \gg \frac{q_m^5}{N^{7/2}} \gg N^{15/4 - 7/2} = N^{1/4}$$

8. Proof of Theorem 2(b)

Let $\sigma > 23/8$. We construct $\alpha = [a_0; a_1, \dots, a_m, \dots]$ which will be of type σ and for which $\limsup R^{(5)}(\alpha, N) = \infty$ by an inductive construction of the partial quotients a_m.

Suppose we have already found $a_0, \dots, a_{m-1}$, from which we got the partial convergents p_j/q_j, $j = 0, \dots, m-1$. Now take an integer $\ell \sim q_{m-1}^{(\sigma-2)/2}$, which is coprime to q_{m-1} (this is certainly possible for $m \gg 1$, say take ℓ a prime between $q_{m-1}^{(\sigma-2)/2}$ and $2q_{m-1}^{(\sigma-2)/2}$ which does not divide q_{m-1}). Also set $v_m = \ell$.

Because ℓ and q_{m-1} are coprime, there is a unique solution $t = a_m$ of the congruence

$$tq_{m-1} + q_{m-2} = 0 \mod \ell^2 \tag{8.1}$$

which lies in $[\ell^2, 2\ell^2)$. Then $a_m \sim \ell^2 \sim q_m^{\sigma-2}$, and

$$q_m := a_m q_{m-1} + q_{m-2} \sim q_{m-1}^{\sigma-1} .$$

Thus α is of type $\sigma + \epsilon$ for all $\epsilon > 0$. Moreover q_m is divisible by v_m^2 by (8.1). Thus

$$q_m = u_m v_m^2$$

for some integer u_m, and

$$v_m \sim q_{m-1}^{(\sigma-2)/2} \sim q_m^{(\sigma-2)/(2\sigma-2)}$$

Now take

$$N_m \sim \frac{q_m^{\sigma/3}}{\log q_m}$$

We will see that $R^{(5)}(\alpha, N_m) \to \infty$ as $m \to \infty$.

To see this, note that in the sequence $\{\alpha n^2 : n \le N_m\}$ we may replace α by the partial convergent p_m/q_m without changing the limiting correlations. To see this, note that by Lemma 5 it suffices to check that $1/q_m q_{m+1} = o(1/N_m^3)$. Indeed, we have

$$\frac{1}{q_m q_{m+1}} \sim \frac{1}{q_m^\sigma} \ll \frac{1}{N_m^3 (\log N_m)^3}$$

as required.

To see that $R^{(5)}(N_m, \frac{p_m}{q_m}, f)$ diverges for positive test functions f with $f(0) \neq 0$, use the divergence principle (4.1) to find

$$R^{(5)}(N_m, \frac{p_m}{q_m}, f) \gg \frac{1}{N_m} (\frac{N_m v_m}{q_m})^5 .$$

Now use $N_m \sim q_m^{\sigma/3}/\log q_m$ and $v_m \sim q_m^{(\sigma-2)/(2\sigma-2)}$ to find

$$R^{(5)}(N_m, \frac{p_m}{q_m}, f) \gg \frac{q_m^E}{(\log q_m)^5}$$

where

$$E = \frac{4\sigma}{3} + 5\frac{\sigma-2}{2\sigma-2} - 5 = \frac{\sigma(8\sigma-23)}{6(\sigma-1)} .$$

Since $\sigma > 23/8$, we have $E > 0$ which gives divergence of $R^{(5)}$. □

9. Proof of Theorem 3

Fix $m \geq 2$, f and $\delta > 0$. By approximating $f(0, x_2, \cdots, x_m)$ from above and below with step functions we see that it is enough to prove the statement for a function f symmetric, satisfying $f(x + (t, t, \cdots, t)) = f(x)$ for all $t \in \mathbf{R}$ and such that $f(0, x_2, \cdots, x_m)$ is the characteristic function of a nice compact set $I \subset \mathbf{R}^{m-1}$. In other words, given such an I and m, δ as above, it is enough to show that as $q \to \infty$ one has

$$R^{(m)}(N, b/q, I) \to Vol(I) \tag{9.1}$$

uniformly for $(b, q) = 1$ and $q^{1-\frac{1}{2m}+\delta} \leq N \leq \frac{q}{\log q}$, where $NR^{(m)}(N, b/q, I)$ is the number of tuples $(x_1, \cdots, x_m)$ with distinct components $x_1, \cdots, x_m$ in $\{1, \cdots, N\}$ such that

$$N(\{\frac{bx_1^2}{q}\} - \{\frac{bx_2^2}{q}\}, \cdots, \{\frac{bx_{m-1}^2}{q}\} - \{\frac{bx_m^2}{q}\}) \in I.$$

Given a large prime number q and b, N as above, we write $R^{(m)}(N, b/q, I)$ in the form

$$R^{(m)}(N, b/q, I) = \frac{1}{N} \sum_{\vec{a} \in sI}^{*} \nu(N, \vec{a})$$

where $s = \frac{q}{N}$ is the dilate factor, and

$$\nu(N, \vec{a}) = \#\{1 \leq x_i \leq N : bx_i^2 - bx_{i+1}^2 = a_i \pmod q, 1 \leq i \leq m-1\} .$$

Here $\sum^*$ means the summation is over the vectors $\vec{a}$ for which the partial sums $A_i = \sum_{k \geq i} a_k, A_m = 0$, are distinct, a condition which comes from the requirement that the m-tuples $x = (x_1, ..., x_m)$ to be counted in $R^{(m)}(N, b/q, I)$ have distinct components. Let

$$h_{\vec{a}}(\vec{x}) = \begin{cases} 1, & b(x_i^2 - x_{i+1}^2) = a_j \pmod q, \qquad i = 1, \cdots, m-1 \\ 0 & \text{else.} \end{cases}$$

Thus:

$$\nu(N,\vec{a}) = \sum_{1\le x_1,\cdots,x_m\le N} h_{\vec{a}}(\vec{x})\ .$$

We now use the Fourier expansion:

$$\nu(N,\vec{a}) = \sum_{\vec{r} \pmod q} \hat{h}_{\vec{a}}(\vec{r}) \prod_{i=1}^{m} F_N(r_i)$$

where

$$\hat{h}_{\vec{a}}(\vec{r}) = \frac{1}{q^m} \sum_{\vec{y} \pmod q} h_{\vec{a}}(\vec{y}) e\Big(-\frac{\vec{r}\cdot\vec{y}}{q}\Big)$$

and:

$$F_N(r_i) = \sum_{1\le x_i\le N} e\Big(\frac{r_i x_i}{q}\Big).$$

These last sums are geometric series which can be bounded by:

$$\|F_N(r_i)\| \ll \min\{N, \frac{q}{|r_i|}\} \tag{9.2}$$

where the residues r_i are assumed to lie in the interval $[\frac{-q}{2}, \frac{q}{2}]$. In

$$R^{(m)}(N, b/q, I) = \frac{1}{N} \sum_{\vec{a}\in sI} \sideset{}{^*}\sum_{\vec{r} \pmod q} \hat{h}_{\vec{a}}(\vec{r}) \prod_{i=1}^{m} F_N(r_i)$$

we isolate the contribution of $\vec{r} = 0$ to get the main term :

$$R^{(m)}(N, b/q, I) = \mathcal{M} + \mathcal{E} \tag{9.3}$$

with

$$\mathcal{M} = N^{m-1} \sideset{}{^*}\sum_{\vec{a}\in sI} \hat{h}_{\vec{a}}(0) \tag{9.4}$$

and

$$\mathcal{E} = \frac{1}{N} \sum_{0\ne\vec{r} \pmod q} \prod_{i=1}^{m} F_N(r_i) \sideset{}{^*}\sum_{\vec{a}\in sI} \hat{h}_a(\vec{r}). \tag{9.5}$$

We first estimate the main term. For any $\vec{a}$ let $C(\vec{a}, q)$ be the curve mod q given by the system of congruences:

$$\begin{aligned} &bx_1^2 - bx_2^2 = a_1 \pmod q \\ &\cdots \\ &bx_{m-1}^2 - bx_m^2 = a_{m-1} \pmod q. \end{aligned}$$

One has $\hat{h}_{\vec{a}}(0) = \frac{1}{q^m}\nu(\vec{a}, q)$, where $\nu(\vec{a}, q)$ is the number of points on the curve $C(\vec{a}, q)$. Thus

$$\mathcal{M} = \frac{N^{m-1}}{q^m} \sideset{}{^*}\sum_{\vec{a}\in sI} \nu(\vec{a}, q). \tag{9.6}$$

We want to show that as $q \to \infty$ one has:

$$\mathcal{M} = Vol(I) + o(1). \tag{9.7}$$

For any $\vec{a} = (a_1, \cdots, a_{m-1})$ denote by $r_{eff}(\vec{a}, q)$ the number of distinct y_j satisfying the following system:

$$y_i - y_{i+1} = a_i(\mod q), 1 \leq i \leq m-1. \tag{9.8}$$

Since the solutions of the homogeneous system

$$y_i - y_{i+1} = 0(\mod q), 1 \leq i \leq m-1$$

are spanned by $(1, \cdots, 1)$, $r_{eff}(\vec{a}, q)$ is well-defined (independent of the particular solution y of (9.8)). Using the Riemann Hypothesis for curves over finite fields (Weil [15]) one obtains (see also [12], Proposition 4):

$$\nu(\vec{a}, q) = 2^{m-r_{eff}(a,q)}(q + B(\vec{a}, q)) \tag{9.9}$$

with

$$|B(\vec{a}, q)| \ll_m q^{\frac{1}{2}}. \tag{9.10}$$

We define roots $\sigma_{ij}(\vec{a})$,$1 \leq i < j \leq m$ by

$$\sigma_{ij}(\vec{a}) = \sum_{k=i}^{j-1} a_k \tag{9.11}$$

so that $\sigma_{i,i+1}(\vec{a}) = a_i$, $\sigma_{ij} = \sum_{k=i}^{j-1} \sigma_{k,k+1}$. We set $D(\vec{a}) = \prod_{1\leq i\leq j\leq m} \sigma_{ij}(\vec{a})$. The solutions of (9.8) are all distinct (i.e. $r_{eff}(\vec{a}, q) = m$) if and only if q does not divide $D(\vec{a})$, since $y_i - y_j = \sum_{k=i}^{j-1} y_k - y_{k+1} = \sum_{k=i}^{j-1} a_k = \sigma_{ij}(\vec{a})$. Note that $D(\vec{a})$ is a nonzero integer for any $\vec{a}$ which appears in the above summations $\sum^*_{a\in sI}$. In our case q does not divide $D(\vec{a})$, since for N large enough in terms of I each factor $\sigma_{i,j}(\vec{a})$ of $D(\vec{a})$ is in absolute value smaller than q. Therefore $r_{eff}(\vec{a}, q) = m$ and (9.9) and (9.10) give

$$\nu(\vec{a}, q) = q + O_m(q^{\frac{1}{2}}) \tag{9.12}$$

for all $\vec{a}$ which appear in (9.6). Then (9.6) implies that

$$\mathcal{M} = \frac{N^{m-1}}{q^m}(q + O_m(q^{\frac{1}{2}}))\sideset{}{^*}\sum_{a\in sI} 1 = \frac{1}{s^{m-1}}(1 + O_m(\frac{1}{q^{\frac{1}{2}}}))\sideset{}{^*}\sum_{a\in sI} 1. \tag{9.13}$$

The number of integer points $\vec{a} \in sI$ which lie in the union of the hyper-planes $\sigma_{ij}(\vec{a}) = 0$ is $O_{m,I}(s^{m-2})$, while by the Lipschitz principle (see Davenport [8]) it follows that:

$$\#(sI \cap \mathbf{Z}^{m-1}) = s^{m-1}Vol(I) + O_{m,I}(s^{m-2}).$$

Therefore:

$$\begin{aligned}\sideset{}{^*}\sum_{a\in sI} 1 &= \#(sI \cap \mathbf{Z}^{m-1}) - \#\{\vec{a} \in sI : D(\vec{a}) = 0\} \\ &= s^{m-1}Vol(I) + O_{m,I}(s^{m-2})\end{aligned} \tag{9.14}$$

and from (9.13) we get

$$\mathcal{M} = (1 + O_m(\frac{1}{\sqrt{q}}))(1 + O_{m,I}(\frac{1}{s}))$$

which proves (9.7).

We now proceed to estimate the remainder $\mathcal{E}$. For any $\vec{a}$ and $\vec{r}$ we have:

$$\hat{h}_{\vec{a}}(\vec{r}) = \frac{1}{q^m}\sum_{\vec{y}\in C(\vec{a},q)} e\Big(-\frac{\vec{r}\cdot\vec{y}}{q}\Big).$$

Applying Weil's Riemann Hypothesis for curves over finite fields one has (see [4], Theorem 6)

$$\Big|\sum_{y\in C(a,q)} e\Big(-\frac{\vec{r}\cdot\vec{y}}{q}\Big)\Big| \ll_m \sqrt{q} \tag{9.15}$$

unless the linear form $\vec{r}\cdot\vec{y}$ is constant along the curve. For $\vec{a}$ as in (9.5) this only happens if $\vec{r} = 0$. For, let $\vec{r} \neq 0$ be such that $\vec{r}\cdot\vec{y}$ is constant along the curve. Then, in the function field $\bar{\mathbf{F}}_q(Y_1, \cdots, Y_m)$ of the curve, where $\bar{\mathbf{F}}_q$ denotes the algebraic closure of $\mathbf{F}_q = \mathbf{Z}/q\mathbf{Z}$, Y_1 is a variable and $Y_2, \cdots, Y_m$ are algebraic functions such that

$$Y_i^2 = Y_1^2 - \frac{a_1 + \cdots + a_{i-1}}{b}$$

for $2 \leq i \leq m$, we will have an equality $\vec{r}\cdot\vec{Y} = c$, with $c \in \bar{\mathbf{F}}_q$. If we choose $j_0 \in \{1, \cdots, m\}$ such that $r_{j_0} \neq 0$ then Y_{j_0} will lie in $\bar{\mathbf{F}}_q(Y_1, \cdots, Y_{j_0-1}, Y_{j_0+1}, \cdots, Y_m)$ and hence

$$\bar{\mathbf{F}}_q(Y_1, \cdots, Y_m) = \bar{\mathbf{F}}_q(Y_1, \cdots, Y_{j_0-1}, Y_{j_0+1}, \cdots, Y_m). \tag{9.16}$$

Now for any unique factorization domain D of characteristic $\neq 2$ and any distinct primes $p_1, \cdots, p_t$ in D one has

$$[K(\sqrt{p_1}, \cdots, \sqrt{p_t}) : K] = 2^t$$

where K denotes the quotient field of D (see Besicovitch [3])). Applying this with $D = \bar{\mathbf{F}}_q[Y_1]$ and $p_i = Y_1^2 - \frac{a_1+\cdots+a_i}{b}$ for $1 \leq i \leq m-1$ we get:

$$[\bar{\mathbf{F}}_q(Y_1, \cdots, Y_m) : \bar{\mathbf{F}}_q(Y_1)] = 2^{m-1}.$$

By the same argument we see that

$$[\bar{\mathbf{F}}_q(Y_1, \cdots, Y_{j_0-1}, Y_{j_0+1}, \cdots, Y_m) : \bar{\mathbf{F}}_q(Y_1)] = 2^{m-2}$$

which contradicts (9.16). It follows that for all $\vec{r}$ and $\vec{a}$ which appear in (9.5), the inequality (9.15) holds true and one has:

$$|\hat{h}_{\vec{a}}(\vec{r})| \ll_m \frac{1}{q^{m-\frac{1}{2}}}.$$

This implies that

$$|\mathcal{E}| \ll_m \frac{1}{Nq^{m-\frac{1}{2}}} \sum_{0 \neq \vec{r} \pmod q} \Big(\prod_{i=1}^{m} |F_N(r_i)| \Big) \sideset{}{^*}\sum_{\vec{a} \in sI} 1. \tag{9.17}$$

We use (9.2) and (9.14) in (9.17) to conclude that

$$|\mathcal{E}| \ll_{m,I} \frac{s^{m-1}}{Nq^{m-\frac{1}{2}}} \sum_{\vec{r} \pmod q} \prod_{i=1}^{m} \min\{N, \frac{q}{|r_i|}\} \tag{9.18}$$

$$\ll_m \frac{q^{m-\frac{1}{2}} \log^m q}{N^m} \leq \Big(\frac{\log q}{q^\delta} \Big)^m.$$

The theorem now follows from (9.3), (9.7) and (9.18).

Appendix A. Square factors of rational approximants

Let α be a real number and a_n/q_n a sequence of rational approximants of α: $|\alpha - a_n/q_n| < 1/q_n^2$, and $q_n \to \infty$. In view of Theorem 1', we want to investigate the square parts of the denominators q_n, keeping in mind that large square parts rule out Poisson statistics for the correlation functions.

Definition A.1. A sequence $\{q_n\}$ is *almost square-free* if $\forall \epsilon > 0$, all square divisors s_n^2 of q_n satisfy $s_n \ll_\epsilon q_n^\epsilon$.

A.1. **A metric result.** We will show that for almost all α, we have: If a_n/q_n is a sequence of rational approximants of α (that is $|\alpha - a_n/q_n| < 1/q_n^2$, and $q_n \to \infty$), then $\{q_n\}$ is almost square-free.

In fact, we show more: For an integer $q \geq 1$, we write $q = \tilde{q}s^2$ with $\tilde{q}$ square-free. Let $\mathcal{F}$ be the set of integers q whose largest square factor s^2 satisfies $s \leq \log^2 \tilde{q}$. We will show that almost all reals α have rational approximants whose denominators are in $\mathcal{F}$ except for finitely many exceptions.

Proposition 7. *For all reals α outside a set of measure zero, there is a $Q = Q(\alpha) > 1$ so that if $|\alpha - a/q| < 1/q^2$ and $q \geq Q$ then $q \in \mathcal{F}$.*

The proof of this follows from a well-known general principle: Given a sequence of integers $\mathcal{N}$, we say that a real number α is $\mathcal{N}$-approximable if there are *infinitely many* rationals $a/q \neq \alpha$ with denominator $q \in \mathcal{N}$ and $|\alpha - a/q| < 1/q^2$. For instance, we may take as $\mathcal{N}$ the complement of $\mathcal{F}$. To prove Proposition 7, we will use

Lemma 8. *Suppose that $\mathcal{N}$ is a sequence such that*

$$\sum_{q \in \mathcal{N}} \frac{1}{q} < \infty.$$

Then the set of $\mathcal{N}$-approximable reals has measure zero.

Proof. Without loss of generality we will assume that $0 < \alpha < 1$. For each pair of coprime integers (a, q) with $1 \leq a < q$, denote by $I_{a,q}$ the interval

$$I_{a,q} = (\frac{a}{q} - \frac{1}{q^2}, \frac{a}{q} + \frac{1}{q^2})$$

Then α is $\mathcal{N}$-approximable if and only if it lies in infinitely many of the intervals $I_{a,q}$ with $q \in \mathcal{N}$. That is for all $N \geq 1$, α lies in

$$M_N := \cup_{N \leq q \in \mathcal{N}} \cup_{1 \leq a < q} I_{a,q}.$$

Thus we need to compute the measure of $M := \cap_{N \geq 1} M_N$. Since $M_N \supseteq M_{N+1} \supseteq \ldots$, we have

$$\text{meas}(M) = \lim_N \text{meas}(M_N) \leq \lim_N \sum_{N \leq q \in \mathcal{N}} \sum_{a=1}^{q} \text{meas}(I_{a,q}) \ll \lim_N \sum_{N \leq q \in \mathcal{N}} \frac{1}{q}$$

(allowing overlap of the intervals). Since $\sum_{q \in \mathcal{N}} 1/q < \infty$, the above limit is zero. □

Thus to prove Proposition 7, it suffices to show

$$\sum_{q \notin \mathcal{F}} \frac{1}{q} < \infty \ .$$

We rewrite this sum by grouping together those q with the same square-free kernel $\tilde{q}$: Writing $q = fm^2$, $\tilde{q} = f$, then

$$\sum_{q\notin\mathcal{F}} \frac{1}{q} = \sum_{f \text{ square-free}} \sum_{\substack{\tilde{q}=f \\ q\notin\mathcal{F}}} \frac{1}{q} = \sum_{f \text{ square-free}} \frac{1}{f} \sum_{q=fm^2\notin\mathcal{F}} \frac{1}{m^2}$$

Now if $q \notin \mathcal{F}$, $\tilde{q} = f$ then $m > \log^2 f$. Thus for each f,

$$\sum_{q=fm^2\notin\mathcal{F}} \frac{1}{m^2} = \sum_{m>\log^2 f} \frac{1}{m^2} \ll \frac{1}{\log^2 f}$$

and so

$$\sum_{q\notin\mathcal{F}} \frac{1}{q} \ll \sum_{f \text{ square-free}} \frac{1}{f}\frac{1}{\log^2 f} < \infty$$

as required. □

A.2. **Algebraic α.** For real *algebraic* α, the analogue of Proposition 7 follows from a standard belief in diophantine analysis, namely the "ABC Conjecture" of Masser and Oesterle: Define the *radical* of an integer N as the product of all primes dividing it: $\mathrm{rad}(N) := \prod_{p|N} p$. The ABC conjecture is the assertion that whenever we have an equation in coprime integers $A + B + C = 0$, then

$$|A| \ll_\epsilon \mathrm{rad}(ABC)^{1+\epsilon} \tag{A.1}$$

for all $\epsilon > 0$. This implies a seemingly stronger statement: Suppose that $G(x, y) \in \mathbf{Z}[x, y]$ is a homogeneous form with integer coefficients and no repeated factors, and m, n coprime integers. Then for all $\epsilon > 0$

$$\max(|m|, |n|)^{\deg(G)-2-\varepsilon} \ll_\epsilon \mathrm{rad}(G(m, n)) \ , \tag{A.2}$$

where $\deg(G)$ is the degree of G. The deduction of (A.2) from (A.1) and a theorem of Belyi [1] was noted by Elkies [9] and by Langevin [13]. The ABC-conjecture (A.1) is the special case of the ternary form $G(x, y) = xy(x + y)$.

The corollary (A.2) of the ABC conjecture implies the analogue of Proposition 7 for irrational algebraic α. Indeed, let $f(x)$ be the minimal polynomial of α, of degree $d > 1$, and write $f(x/y) = F(x, y)/y^d$ with $F(x, y) \in \mathbf{Z}[x, y]$. Suppose that p/q is an approximant of α: $|\alpha - p/q| < 1/q^2$, with p, q coprime. Since $f(x)$ is irreducible, $f'(\alpha) \neq 0$ and thus by the mean value theorem, for some ξ between α and p/q,

$$|f(\frac{p}{q})| = |f(\frac{p}{q}) - f(\alpha)| = |\alpha - \frac{p}{q}||f'(\xi)| \ll \frac{1}{q^2}$$

On the other hand,

$$f(\frac{p}{q}) = \frac{F(p,q)}{q^d}$$

and so we find

$$|F(p,q)| \ll q^{d-2} .$$

By (A.2), taking $G(x,y) = xyF(x,y)$ and noting that $|p| \ll q$, we get for all $\epsilon > 0$

$$q^{d-\epsilon} \ll_\epsilon \operatorname{rad}(pqF(p,q)) \leq |pF(p,q)| \operatorname{rad}(q) \ll q^{d-1} \operatorname{rad}(q) .$$

Thus if $q = \tilde{q}s^2$ then

$$(\tilde{q}s^2)^{d-\epsilon} \ll_\epsilon \operatorname{rad}(\tilde{q}s) \leq \tilde{q}s$$

and so $s \ll_\epsilon q^\epsilon$.

References

[1] G. V. Belyi, *Galois extensions of a maximal cyclotomic field* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 2, 267–276, 479

[2] M. V. Berry and M. Tabor, *Level clustering in the regular spectrum*, Proc. Royal Soc. London A356(1977), 375-394

[3] A.S. Besicovitch, *On the linear independence of fractional powers of integers*, J. London Math. Soc. **15** (1940), 3–6.

[4] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. **88** (1966) , 71–105.

[5] G. Casati, I. Guarneri and F. M. Izrailev, *Statistical properties of the quasi-energy spectrum of a simple integrable system*, Phys. Lett. A 124(1987), 263–266.

[6] H. Davenport, *On the distribution of quadratic residues (mod p)* Jour. London Math. Soc. **6** (1931), 49–54, *ibid.* **8** (1933), 46–52.

[7] ———, *On character sums in finite fields*, Acta Math. **71** (1939), 99-121.

[8] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183. Corrigendum: "On a principle of Lipschitz". J. London Math. Soc. **39** (1964), 580.

[9] N. Elkies, *ABC implies Mordell*, Internat. Math. Res. Notices 1991, no. 7, 99–109.

[10] W. Feller, *An introduction to probability theory and its applications*, Vol. II. Second edition John Wiley & Sons, Inc., New York-London-Sydney 1971.

[11] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, The Clarendon Press, Oxford University Press, New York, 1979.

[12] P. Kurlberg and Z. Rudnick, *The distribution of spacings between quadratic residues*, Duke Math. Jour. **100** (1999), 211-242.

[13] M. Langevin, *Partie sans facteur carre de $F(a,b)$ (modulo la conjecture abc)*, Seminaire de Theorie des Nombres (1993–1994), Publ. Math. Univ. Caen.

[14] Z. Rudnick and P. Sarnak, *The pair correlation function of fractional parts of polynomials*, Comm. in Math. Physics. **194** (1998), 61–70.

[15] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann. Paris 1948.

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel (rudnick@math.tau.ac.il)

Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ, 08544, USA (sarnak@math.princeton.edu)

Department of Mathematics, University of Illinois, 1409 West Green Street, Urbana, IL 61801, USA (zaharesc@math.uiuc.edu)